Privacy in Europe: An Overview and Update on the EU-US Dialogue

1. Privacy in Europe – A Sensitive Subject

Since the *judgment* of the Court of Justice of the European Union (CJEU) on October 6, 2015 in *Maximillian Schrems vs Data Protection Commissioner*, the EU and US have stepped up their efforts to ensure continued transatlantic transfers of personal data. The debate has been heated and is still not settled.

This briefing summarises the current EU legal position, reports on the latest results of the EU-US dialogue and comments on how companies can comply in the future.

2. The Genesis of the Right to Privacy

First, however, why are Europeans so exercised about protection of personal data and privacy? A good place to start is the European Convention on Human Rights, which was adopted in 1950 – just as the Cold War became apparent and only five years after the end of the Second World War – and as a direct consequence of the adoption of the UN Universal Declaration of Human Rights. Article 8 of the 1950 version of the Convention states,

> "*(1) Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> *(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or other economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*"

Article 8 has been the basis for the right to protection of personal data, in particular the 1980 "Convention of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data". In the same year, the Organization of Economic Cooperation and Development (OECD) codified its "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data". In the EU, these texts culminated in the 1995 Data Protection Directive. More recently, the "Charter of Fundamental Rights of the European Union" reaffirms rights to privacy and protection of personal data. Article 7 enshrines "*the right to respect for his or her private and family life, home and communications*", while Article 8 provides,

> "*1. Everyone has the right to the protection of personal data concerning him or her.*
>
> *2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
>
> *3. Compliance with these rules shall be subject to control by an independent authority.*"

Societies that share comparable rights and values develop comparable responses: for the US see, for example, "Fair Information Practice Principles" discussed in the US Department of Health, Education and Welfare's 1973 report and enshrined in the Privacy Act of 1974.

These principles exist to protect citizens from the grim realities of totalitarianism. One of many striking examples within living memory in Europe is the East German secret police, the Stasi, which, over a forty-year period, amassed a huge amount of data about East German citizens - about 17 million people. Even after destruction by the Stasi of numerous files, there still remains about: 111 kilometres of written files (including 12 kilometres of card indexes) and comprising some 41 million individual files; microfilms which, if printed, would make up 47 kilometres; 1.7 million photos; 27,300 audio documents; 2,800 films and videos; and some 15,000 boxes and bags of documents that had been torn by hand by Stasi members during the collapse of East Germany in 1989/1990. This is a staggering and chilling "achievement" for a period that largely pre-dated the IT revolution and its exponential computing power.

A July 2015 Eurobarometer survey provides another perspective, for example,

> "*Only a minority (15%) feel they have complete control over the information they provide online; 31% think they have no control over it at all.*
>
> *Two-thirds of respondents (67%) are concerned about not having complete control over the information they provide online.*
>
> *Half of Europeans have heard about revelations concerning mass data collection by governments. Awareness ranges from 76% in Germany to 22% in Bulgaria.*
>
> *Over half of respondents* ***disagree*** *with the statement, "providing personal information is not a big issue for you" (57%).*
>
> *Nine out of ten Europeans think that it is important for them to have the same rights and protection over their personal information, regardless of the country in which the public authority or private company offering the service is based.*
>
> *69% of people say they their explicit approval should be required in all cases before their data is collected and processed.*
>
> *Roughly seven out of ten people are concerned about their information being used for a different purpose from the one it was collected for.*
>
> *When asked who they think should make sure the personal information they provide online is collected, stored and exchanged safely, respondents believe the responsibility is shared between online companies (67%) and individuals themselves (66%), but also public authorities (55%).*"

3. Current EU Law

Against the above troubling background, current EU law – primarily the 1995 Data Protection Directive – requires processing of personal data to have a legal basis: (i) the individual's consent; (ii) performance of a contract; (iii) compliance with a legal obligation; (iv) protection of vital interests of the individual; (v) public interest; and (vi) legitimate interests pursued by the controller or a third party. Furthermore, the processing must have a defined purpose. Individuals enjoy rights, such as access to their personal data, to object to processing and to rectify data.

Logically, transfers of personal data outside the EU are also subject to legal safeguards: the third country must ensure an adequate level of protection. The Commission is mandated to find that a third country ensures adequate protection. To do so, it must assess adequacy in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations. It must also consider in particular: the nature of the data; the purpose and duration of the proposed processing operation or operations; the country of origin and country of final destination; the rules of law, both

general and sectoral, in force in the third country in question; and the professional rules and security measures which are complied with in that country.

In 2000, the Commission's assessment of the US enabled it to adopt its "Safe Harbour" decision. What worked in 2000 was not, however, destined to last forever and, in its *Schrems* ruling, the European Court held the decision to be invalid with effect from October 6, 2015.

One particular aspect of the judgment covered the Commission's failure to demonstrate that it had reviewed the national security/law enforcement exception in the Safe Harbour principles which would enable (mass) surveillance. Based on the evidence provided to the Court, the judges could not comment on whether there were sufficient legal constraints in US law to safeguard EU citizens from mass surveillance by US authorities. The Court held that if the Commission were to adopt a new decision, both the exception and the safeguards would be essential aspects for the Commission to examine.

4. A New Framework for Transatlantic Transfers

The US and EU authorities have been working since then to address the consequences of the Court's judgment. On February 2, the European Commission and US Department of Commerce announced that they had finalised a new framework for transatlantic data transfers. Known as the "EU-US Privacy Shield" it is intended to replace Safe Harbour. For that to happen, the Commission must decide whether, following its assessment of US law and practice, the US provides adequate protection for personal data. At that point, the full text on Privacy Shield will be made available.

As has been widely reported, there have been major changes to US legislation regarding data privacy - Presidential Policy Directive/PPD-28 – in particular, following the Snowden revelations. According to this directive, companies are now required to report periodically on Government Information Requests through transparency reports, for example, see http://www.apple.com/privacy/transparency-reports/ https://transparency.twitter.com/ https://www.google.com/transparencyreport/.

Privacy Shield will introduce two new safeguards. The first relates to surveillance activities by the government. A new ombudsman, based in the State Department, will have direct access to the intelligence agencies' independent inspectors-general which were set up under PPD-28. This should enable individuals to complain about government surveillance. It will not, however, give them similar rights to those they enjoy under EU legislation *e.g.* to access, rectify or require erasure of data, or to object to processing. Their complaints will be investigated according to US administrative rules and US law.

The second safeguard covers misuse of personal data by companies that adhere to the Privacy Shield voluntary scheme. A new arbitration system will be set up, under the Federal Arbitration Act, to act as a last resort to resolve conflicts between EU data subjects and Privacy Shield companies. This will provide the judicial redress for EU data subjects which was lacking under Safe Harbour. It will not, however, be available for complaints based on government access to company data: the new ombudsman should address these. The US Department of Commerce has released a fact sheet with additional points.

Member State data protection authorities (DPAs), sitting as the Article 29 Working Party, have given a cautious welcome to the new deal. They will hold an extraordinary meeting at the end of March to assess whether the US framework meets the four guarantees on intelligence activities, as prescribed in the *Schrems* judgment, namely: clear, precise and predictable rules; necessity and proportionality; independent oversight mechanisms; and availability of effective remedies for individuals (defence of rights before an independent body). The Working Party still has concerns about the scope of surveillance in the US and the remedies proposed. They will also examine whether the provisions respect the powers of the DPAs. Meantime, they agree to transfers continuing on other bases contemplated by the 1995 Directive, namely "model contractual clauses" (MCCs) or "binding corporate rules" (BCRs).

There are many unanswered questions at this stage. These include the following:

- It is not clear whether the companies that are currently under Safe Harbour would have to join Privacy Shield or would enjoy "grandfather" rights: since the Privacy Shield has to be materially different from Safe Harbour in order to ensure its validity (and reduce the risk of legal challenge), it seems likely that companies will have to apply to join, possibly under a streamlined procedure.

- The length of the transition period between the two schemes, and the enforcement position during that transition period, are not clear. The Commission must first adopt a decision on the adequacy of US protection. Meantime, it remains uncertain whether Member State DPAs will pursue Safe Harbour companies that have not adopted alternative safeguards such as MCCs. Safe Harbour companies that continue to transfer personal data without alternative safeguards may be at risk of action by national DPAs, particularly if an individual complains, for example significant fines and "naming and shaming" as prescribed under national laws.

- Companies that have BCRs or MCCs are also unsure that these effectively shield them from enforcement action in the longer term, since BCRs and MCCs have a national security/law enforcement exception, which was one of the contentious points in *Schrems*. The Article 29 Working Party has said that these safeguards may be used pending its extraordinary meeting; at that meeting, they will take a view as to their longer-term future. BCRs and MCCs should, therefore, remain valid safeguard tools until, at least, mid-April (the expected date for an adequacy decision) and, arguably, beyond that date. Their continued validity would demonstrate that companies can transfer personal data between the EU and US more effectively than elsewhere.

- Neither the EU (Commission or Article 29 Working Party) nor the US (Department of Commerce) has set out the precise legal position for onward transfers of data. Absent the Privacy Shield text, which is still awaited, it is not possible to ascertain what the regime will be.

- Finally, following the *Schrems* judgment, certain other countries – such as Switzerland and Israel – which had set up their own Safe Harbour arrangements with the US concluded that their arrangements were also invalid and terminated them. The EU-US Privacy Shield may encourage these countries, but does not oblige them, to conclude new arrangements.

5. Creating a Modern EU Legislative Framework

The EU institutions have recognised that the 1995 Directive and its national implementing rules are no longer fit for purpose and, since early 2012, have been negotiating a new text, the General Data Protection Regulation (latest available version) (the GDPR). This text has now been agreed within the Council and is currently before the European Parliament and Council for final adoption. It will not, however, apply until 2018.

The GDPR acknowledges that,

> "*Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of data sharing and collecting has increased spectacularly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Individuals increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.*" (Recital 5)

It furthermore recites,

> "*The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the way data protection is implemented across the Union, legal uncertainty and a widespread public perception that there are significant risks for the protection of individuals associated notably with online activity*." (Recital 7)

The GDPR is a detailed and comprehensive text – over 135 recitals and 91 Articles – whose objectives, as set out in Article 1, are: (i) to lay down rules relating to the protection of individuals with regard to the processing of personal data and rules relating to the free movement of personal data; (ii) to protect fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data; and (iii) to ensure that the free movement of personal data within the EU shall neither be restricted nor prohibited for reasons connected with the protection of individuals with regard to processing of personal data – in other words, a Single Market in personal data, subject to all Member States also protecting fundamental rights, such as privacy.

Like the 1995 Directive, the GDPR regulates transfers of personal data to third countries, but in much more detailed terms. Since it is a regulation – rather than a directive – its terms apply directly in all EU Member States without any need for national implementing rules. This reduces the "patchwork" of national rules: the rules may be stricter, but at least they are uniform.

The GDPR contains several other provisions which are significant in a US-EU context.

First, its broad territorial scope. The GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. It also applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (i) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (ii) the monitoring of their behaviour as far as their behaviour takes place within the EU. The GDPR provides limited guidance to ascertain whether a controller or processor is "targetting" EU data subjects for such goods or services, or monitoring behaviour. (Recitals 20-21 and Article 3)

Second, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should use solutions that provide data subjects with enforceable and effective rights. Transfers should only be allowed where the conditions of the GDPR for a transfer to third countries are met. (Recitals 89-91, Article 40). The GDPR further specifies the criteria that the Commission should take into account for adequacy decisions; decisions will be reviewed at least every four years. Current decisions remain in force until amended, replaced, or repealed. (Recitals 80-82, Article 41)

Third, the GDPR divides the "appropriate safeguards" into two: those that may be used without prior authorisation from DPAs (BCRs, MCCs and codes of conduct are included), and those that may not (bespoke contractual clauses or administrative arrangements between public authorities). Importantly, existing authorisations remain valid until amended, replaced, or repealed. (Recitals 83-84, Article 42)

Fourth, the Commission will adopt an implementing act to develop BCRs further. (Recital 85, Article 43)

Fifth, the GDPR expressly sets out the general international principle that any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the EU or a Member State, without prejudice to other grounds for transfer provided under the GDPR. (Recitals 78-79 and Article 43a)

Finally, the GDPR grants waivers ("derogations") for specific situations (cf. the 1995 Directive): (i) explicit consent by the data subject to the proposed transfer following a warning; (ii) performance of a contract/pre-contractual information on the data subject's request; (iii) performance of a contract concluded in the interest of the data subject between the controller and another; (iv) public interest; (v) establishment, exercise and defence of legal claims; (vi) vital interest of the data subject; (vii) public register; and (viii) introduction of a new "catch-all" with safeguards: "*If the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, where the controller has assessed all the circumstances surrounding the data transfer and based on this assessment adduced suitable safeguards with respect to the protection of personal data. The controller shall inform the [data protection authorities] of the transfer*." The controller must also explicitly inform the data subject about the transfer and the compelling legitimate interests pursued by the controller. (Recitals 86-88, Article 44)

6. Criminal and Security Dimension

The EU institutional framework reflects those competencies which, over the years, the Member States have been willing to entrust to it: initially, creating a Single Market, an economic objective, prevailed – and the 1995 Directive was a product of that objective. In later years, the EU has intervened in core areas of national sovereignty, such as criminal law. It has done so on more tentative, classically intergovernmental bases. For these reasons, the GDPR "…*does not address issues of protection of fundamental rights and freedoms or the free flow of data related to activities which fall outside the scope of Union law, such as activities concerning national security, nor does it cover the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.*" (Recital 14)

Likewise, the EU legislator has proposed a separate text for processing of personal data to prevent crime, namely a proposal for a "Directive on the protection of individuals with regard to processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data". As with the GDPR, this proposal has now been agreed within the Council and is before the Parliament and Council for final adoption. See: Commission press release, December 15, 2015 and Council press release, December 18, 2015 for additional commentary.

7. Next Steps for Companies and Concluding Remarks

To sum up, each of the EU texts referred to above addresses specific objectives, for example the 1995 Directive promotes an EU Single Market in personal data with specific, proportionate and non-discriminatory rules for transfer out of the EU.

Given Europe's history, EU citizens and their governments will remain attentive to privacy and protection of personal data.

For transatlantic businesses, this means that the current position is uncertain: transfers based on Safe Harbour are no longer valid and companies therefore need to consider alternatives, such as: consent of the individual (which must be unambiguous or explicit, depending on the type of personal data being processed); BCRs and MCCs (and even these may be open to challenge); and any of the other bases contemplated by the 1995 Directive listed under "Current EU Law" above. DPAs tend to construe these bases narrowly; as a result, companies need to check their procedures against relevant national laws implementing the 1995 Directive. Some companies may conclude that, to minimize risk of challenge, they must retain personal data in the EU – this is "balkanisation" of a global market in personal data.

Companies also need to monitor progress with the Privacy Shield, in particular following the Article 29 Working Party meeting at the end of March, and on release of the full text by the EU and US authorities. In addition, although the GDPR will not apply until 2018, they need to: (i) integrate its

much more detailed provisions into their policies and procedures now, *i.e.* a "lead-in" time; and (ii) align transfers out of the EU with the GDPR, as well as the Privacy Shield and any other basis, such as MCCs.

Finally, none of the above prevents or restricts third countries, such as the US, requesting assistance in accordance with appropriate legal bases, to combat terrorism. Other legal texts govern such requests, for example the "Umbrella agreement" awaiting signature between the EU and US and the Terrorist Finance Tracking Programme. Other examples include the US-EU agreement on passenger name records and ESTA, the US visa waiver programme. This case-by-case approach is more justifiable and proportionate, and less susceptible to challenge - than the legally unsupported mass surveillance identified in the *Schrems* judgment.

No doubt, all will gradually become clearer as the debate unfolds with the next stage being the Article 29 Working Party meeting at the end of March.

Brussels, February 2016

Steptoe
STEPTOE & JOHNSON LLP

Philip Woolfson, Partner
Tel: +32 (2) 626 0519
Mob: +32 475 68 12 16
Email: pwoolfson@steptoe.com

Daniella Terruso, EU Policy Advisor
Tel: +32 (2) 626 0598
Mob: +32 486 53 99 13
Email: dterruso@steptoe.com

Steptoe & Johnson LLP
489 Avenue Louise
B-1050 Brussels, Belgium
Tel: +32 (2) 626 0500
Fax: +32 (2) 626 0510

Maury Shenk, Advisor
Tel: +44 20 7367 8050
Mob: +44 7824 663 680
Email: mshenk@steptoe.com

Steptoe & Johnson
5 Aldermanbury Square
London EC2V 7HR
Tel: +44 20 7367 8000
Fax: +44 20 7367 8001

www.steptoe.com